PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-140302
(43)Date of publication of application : 17.05.2002

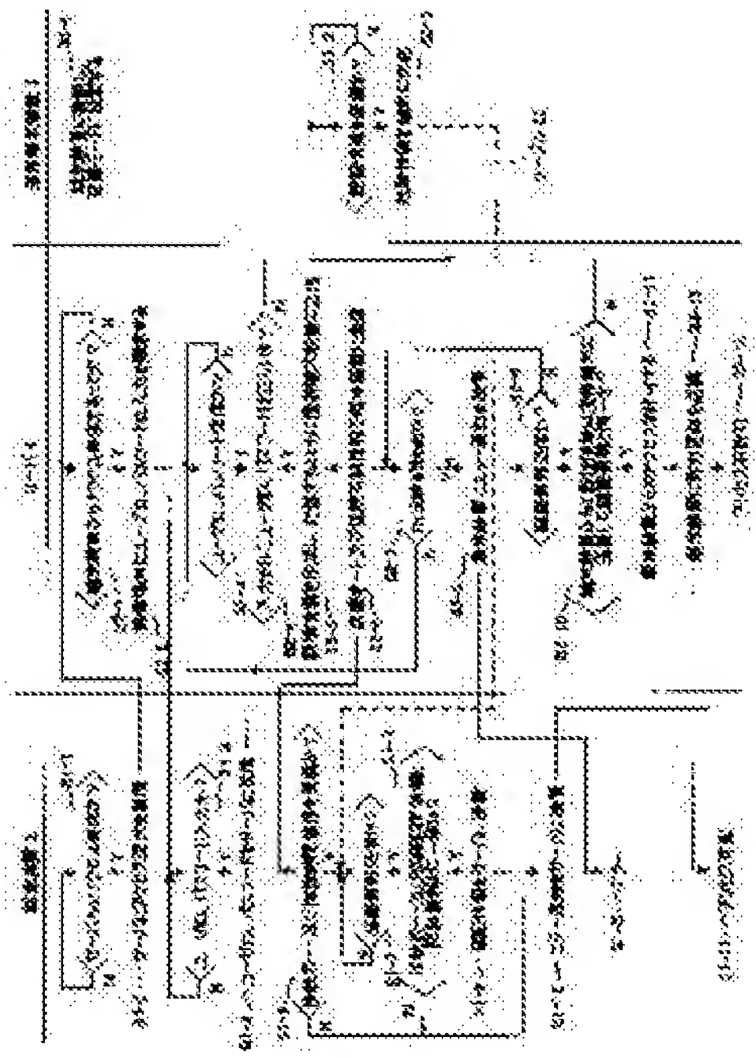
(51)Int.Cl. G06F 15/00
H04L 9/32

(21)Application number : 2000-331353
(22)Date of filing : 30.10.2000

(71)Applicant : HORINAOKI
(72)Inventor : HORINAOKI

(54) METHOD AND DEVICE FOR AUTHENTICATION AND TERMINAL DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a method and a device for authentication and a terminal device which disable a multi-user computer system and a network system to illegally be used with ease when a method and a device for authentication and a terminal for identification when they are used.
SOLUTION: The authenticating device (4) sends prescribed information to a previously registered 2nd terminal device (3) at an authentication request from a 1st terminal device (2), the 2nd terminal device (3) sends the prescribed information to the 1st terminal device (2), and the specific information from the 2nd terminal device (3) is sent back from the 1st terminal device (2) to the authenticating device; and the authenticating device (4) compares the information sent back from the 1st terminal device (2) with the information sent out to the 2nd terminal device (3) and judges the adequacy of the 1st terminal device (3) according to the comparison result.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－140302
（P2002－140302A）
(43)公開日　平成14年５月17日(2002.5.17)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）	
Ｇ０６Ｆ　15/00	３３０	Ｃ０６Ｆ　15/00	３３０Ｃ	５Ｂ０８５
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	５Ｊ１０４

審査請求　未請求　請求項の数７　ＯＬ　（全 14 頁）

(21)出願番号　特願2000－331353(P2000－331353)

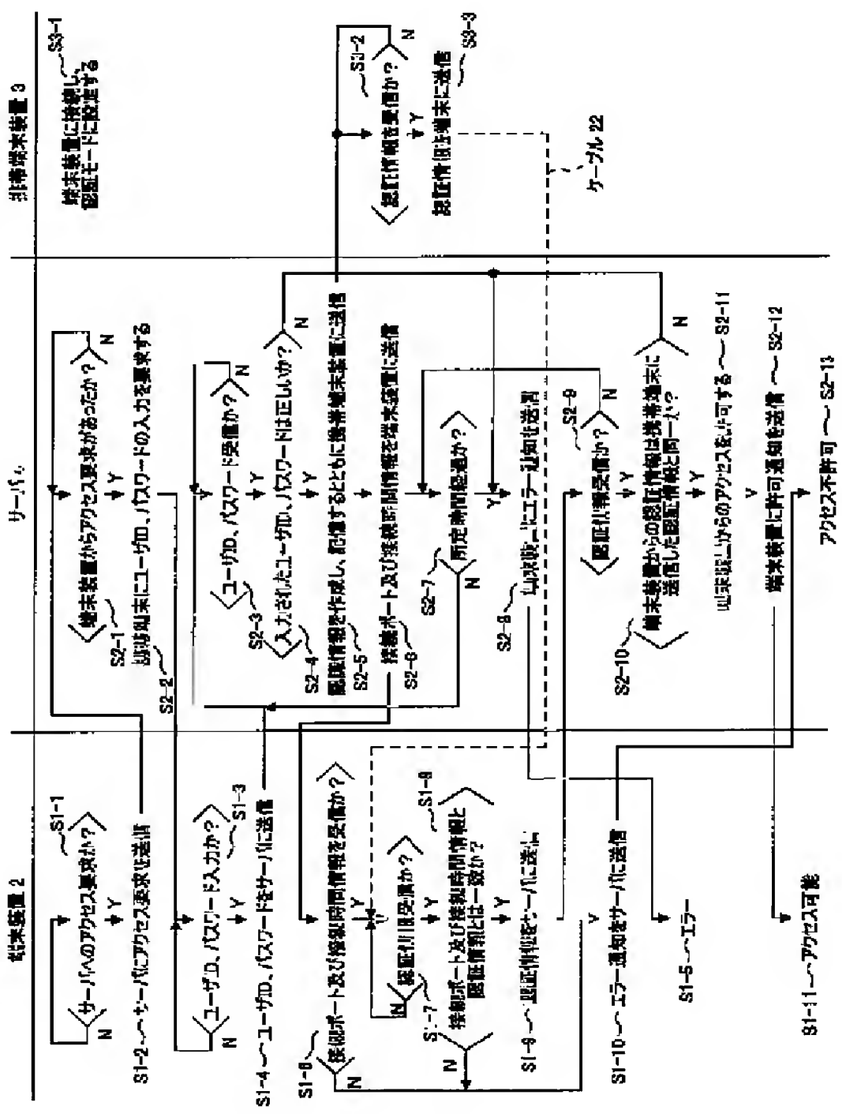
(22)出願日　平成12年10月30日(2000.10.30)

(71)出願人　500503780
堀　直樹
北海道札幌市西区福井８丁目３－６
(72)発明者　堀　直樹
北海道札幌市西区福井８丁目３－６
(74)代理人　100070150
弁理士　伊東　忠彦

Ｆターム(参考)　5B085 AE04 AE23
5J104 AA07 KA01 KA02 KA20 NA05
PA02 PA07

(54)【発明の名称】　認証方法及び認証装置並びに端末装置

(57)【要約】
【課題】　マルチユーザのコンピュータ・システムやネットワーク・システムを使用する際に本人であることを確認するための認証方法及び認証装置並びに端末装置に関し、不正利用を容易に行なえない認証方法及び認証装置並びに端末装置を提供することを目的とする。
【解決手段】　認証装置（４）から、第１の端末装置（２）からの認証要求に応じて予め登録された第２の端末装置（３）に所定の情報を送出し、前記第２の端末装置（３）から前記第１の端末装置（２）に前記所定の情報を送出し、前記第２の端末装置（３）からの前記所定の情報を前記第１の端末装置（２）から前記認証装置に返送し、前記認証装置（４）で、前記第１の端末装置（２）から返送される情報と前記第２の端末装置（３）に送出した前記所定の情報とを比較して、その比較結果に基づいて前記第１の端末装置（３）の正当性を判定する。



【特許請求の範囲】
【請求項１】　認証装置から、第１の端末装置からの認証要求に応じて予め登録された第２の端末装置に所定の情報を送出し、
前記第２の端末装置から前記第１の端末装置に前記所定の情報を送出し、
前記第２の端末装置からの前記所定の情報を前記第１の端末装置から前記認証装置に返送し、
前記認証装置で、前記第１の端末装置から返送される情報と前記第２の端末装置に送出した前記所定の情報とを比較して、その比較結果に基づいて前記第１の端末装置の正当性を判定することを特徴とする認証方法。
【請求項２】　前記第２の端末装置は、現在位置情報を検出し、前記第２の端末装置から前記第１の端末装置に送出する情報に該位置情報を合成して前記第１の端末装置に送出し、
前記認証装置は、前記第１の端末装置から返送される位置情報と、予め登録された位置情報とを比較して、その比較結果に基づいて前記第１の端末装置の正当性を判定することを特徴とする請求項１記載の認証方法。
【請求項３】　第１の端末装置から認証が要求された場合、該第１の端末装置からの認証要求に応じて予め登録された第２の端末装置に所定の情報を送信し、
前記第１の端末装置からの返送情報と前記第２の端末装置への前記所定の情報とを比較し、
前記第１の端末装置からの前記返送情報と前記第２の端末装置への前記所定の情報とで所定の対応がとれたときに、前記第１の端末装置を正当であると判定する認証処理部を有することを特徴とする認証装置。
【請求項４】　前記第２の端末装置は、現在位置を検出し、前記第１の端末装置への情報に合成して前記第１の端末装置に送出し、
前記認証処理部は、予め登録された位置情報と、前記第２の端末装置で合成された位置情報とを比較し、両位置情報の対応がとれたときに、前記第１の端末装置を正当であると判定することを特徴とする請求項３記載の認証装置。
【請求項５】　認証処理状態を設定する設定部と、
前記設定部により認証処理状態が設定された場合に、認証装置から情報を受信したとき、該認証装置からの情報を他の端末装置に送信する認証処理部とを有することを特徴とする端末装置。
【請求項６】　現在位置を示す位置情報を検出する検出部を有し、
前記認証処理部は、前記認証装置からの情報に前記検出部で検出された前記位置情報を付加して前記他の端末装置に送信することを特徴とする請求項５記載の端末装置。
【請求項７】　認証要求時に、他の端末装置から供給される情報を受信し、
前記他の端末装置からの情報を、手動又は自動で認証装置に送信する認証処理部を有することを特徴とする端末装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は認証方法及び認証装置並びに端末装置に係り、特に、マルチユーザのコンピュータ・システムやネットワーク・システムを使用する際に本人であることを確認するための認証方法及び認証装置並びに端末装置に関する。
【０００２】近年、インターネット上でショッピングなどの商取引を行うことができるようになっており、その取引の代金支払いのための手続きにも認証処理が不可欠になっている。このため、安全確実な認証方式が求められている。
【０００３】
【従来の技術】マルチユーザのコンピュータ・システムやネットワーク・システムで個人を認証する際には、通常ユーザＩＤとパスワードの組み合わせによって認証が行われる。
【０００４】例えば、ユーザがコンピュータ・システムやネットワークにログ・インする際に、ユーザＩＤとパスワードの入力が要求される。ユーザが両方のデータを入力すると、それがあらかじめアクセス許可リストに登録されたものかどうかの認証が行なわれ、認証された場合にシステムの使用が許可される。
【０００５】
【発明が解決しようとする課題】しかるに、従来の認証システムは、通常ユーザＩＤとパスワードによってシステムの使用が許可されるため、第三者にユーザＩＤとパスワードとが知られた場合には、第三者がユーザＩＤとパスワードの取得者のユーザになりすましてシステムを使用することができる。このため、第三者に電子メールの内容をのぞかれたり、電子メールの送受信の履歴が見られて、だれとメールのやり取りしているのかなどの情報を知られたりしてしまう。また、第三者により勝手にインターネットやパソコン通信が使用され、覚えのない利用料金を請求されたり、覚えのない物品購入、販売や詐欺行為など不正利用されたりするなどの問題点があった。
【０００６】本発明は上記の点に鑑みてなされたもので、不正利用を容易に行なえない認証方法及び認証装置並びに端末装置を提供することを目的とする。
【０００７】
【課題を解決するための手段】本発明は、認証装置（４）から、第１の端末装置（２）からの認証要求に応じて予め登録された第２の端末装置（３）に所定の情報を送出し、前記第２の端末装置（３）から前記第１の端末装置（２）に前記所定の情報を送出し、前記第２の端末装置（３）からの前記所定の情報を前記第１の端末装

置（２）から前記認証装置に返送し、前記認証装置（４）で、前記第１の端末装置（２）から返送される情報と前記第２の端末装置（３）に送出した前記所定の情報とを比較して、その比較結果に基づいて前記第１の端末装置（３）の正当性を判定するものである。

【０００８】本発明によれば、ユーザＩＤやパスワードを知っているだけでは第１の端末装置（２）は認証されることはなく、第１の端末装置（２）と第２の端末装置（３）とを組み合わせて使用する必要があるため、ユーザＩＤやパスワードの不正使用が困難になる。

【０００９】また、本発明は、前記第２の端末装置（３）で現在位置を検出し、前記第２の端末装置（３）から前記第１の端末装置（２）に送出する情報に前記位置情報を合成して前記第１の端末装置（２）に送出し、前記認証装置（４）で、前記第１の端末装置（２）から返送される前記位置情報と、予め登録された位置情報とを比較して、その比較結果に基づいて前記第１の端末装置（２）の正当性を判定するようにしてなる。

【００１０】本発明によれば、第２の端末装置（３）が認証装置（４）に予め登録された位置に対応する位置にあるときに、第１の端末装置（２）の正当性が判定されるので、ユーザＩＤやパスワードの不正使用をさらに困難にできる。

【００１１】

【発明の実施の形態】図１に本発明の第１実施例のシステム構成図を示す。

【００１２】本実施例のシステム１は、端末装置２、携帯端末装置３、サーバ４、ネットワーク５を含む構成とされている。

【００１３】端末装置２は、例えば、パーソナルコンピュータやゲーム機などから構成されており、ネットワーク５を介してサーバ４にアクセス可能とされている。

【００１４】図２に本発明の第１実施例の端末装置にブロック構成図を示す。

【００１５】端末装置２は、ＣＰＵ１１、ＲＡＭ１２、ＲＯＭ１３、ハードディスクドライブ１４、ＣＤ－ＲＯＭドライブ１５、入力装置１６、表示装置１７、表示コントローラ１８、インタフェースコントローラ１９、モデム２０を含む構成とされている。ＣＰＵ１１は、サーバ４へのアクセス時にハードディスクドライブ１４に予めインストールされた認証用プログラムに基づいて認証処理を行なう。ＲＡＭ１２は、ＣＰＵ１１での処理を実行する際の作業用記憶領域として用いられる。

【００１６】ＣＰＵ１１で実行される認証用プログラムは、例えば、ＣＤ－ＲＯＭ２１に書き込まれてユーザに提供され、ＣＤ－ＲＯＭドライブ１４によりハードディスクドライブ１４にインストールされる。なお、本実施例では、認証用プログラムをＣＤ－ＲＯＭ２１により提供するようにしたが、フロッピー（登録商標）ディスク、光磁気ディスク、他の光ディスクなど他の記録媒体で提供するようにしてもよい。また、所定のサーバからネットワークを介して提供するようにしてもよい。

【００１７】インタフェースコントローラ１９は、携帯端末装置３にケーブル２２を介して接続され、携帯端末装置３との通信制御を行ない、認証処理時には、携帯端末装置３から認証情報が供給される。モデム２０は、ネットワーク５との通信制御を行うものであり、サーバ４にアクセス要求を送信するとともに、認証処理時にはサーバ４に認証情報を送信する。インタフェースコントローラ１９は、携帯端末装置３にケーブル２２を介して接続され、携帯端末装置３との通信制御を行なうものであり、認証処理時には、携帯端末装置３から認証情報が供給される。

【００１８】なお、ＲＯＭ１３には、ＢＩＯＳ（Basic Input/Output System）が記憶されている。また、表示装置１７は、表示コントローラ１８により制御され、文字やグラフィックスなどの表示を行なう。

【００１９】携帯端末装置３は、携帯電話機やＰＨＳ（Personal Handy Phone System）電話機などから構成されており、認証モード設定時にはサーバ４からネットワーク５を介して認証情報を受信し、受信した認証情報をケーブル２２を介して端末装置２に認証情報を送信する。

【００２０】図３に本発明の第１実施例の携帯端末装置のブロック構成図を示す。

【００２１】携帯端末装置３は、アンテナ３１、受信部３２、送信部３３、データ処理部３４、インタフェースコントローラ３５、マイクロフォン３６、スピーカ３７、操作部３８を含む構成とされている。

【００２２】アンテナ３１で受信された受信信号は、受信部３２に供給され、元のデータに復調される。受信部３２で復調されたデータは、データ処理部３４に供給される。データ処理部３４は、メモリ３４ａを内蔵しており、このメモリ３４ａには認証プログラムが予め記憶されている。

【００２３】データ処理部３４は、操作部３８の操作により、認証モードに設定されると、認証プログラムを実行する。データ処理部３４で実行される認証プログラムは、サーバ４からの認証情報をインタフェースコントローラ３５、ケーブル２２を介して端末装置２に送信する処理が実行される。また、データ処理部３４は、携帯電話機としての処理を実行する。

【００２４】サーバ４は、端末装置２からのアクセス要求に応じて認証処理を実行し、アクセス要求があった端末装置２が認証されたときに、端末装置２に各種サービスを提供する。

【００２５】次に、サーバ４の構成を説明する。

【００２６】図４に本発明の第１実施例のサーバのブロック構成図を示す。

【００２７】サーバ４は、ＣＰＵ５１、ＲＡＭ５２、Ｒ

ＯＭ５３、ハードディスクドライブ５４、ＣＤ－ＲＯＭドライブ５５、入力装置５６、表示装置５７、表示コントローラ５８、通信コントローラ５９、認証情報データベース６０を含む構成とされている。ＣＰＵ５１は、端末装置２からのアクセス時にハードディスクドライブ５４に予めインストールされた認証プログラムに基づいて認証処理を行なう。ＲＡＭ５２は、ＣＰＵ５１での処理を実行する際の作業用記憶領域として用いられる。

【００２８】認証プログラムは、例えば、ＣＤ－ＲＯＭ６３に書き込まれてユーザに提供され、ＣＤ－ＲＯＭドライブ５４によりハードディスクドライブ５４にインストールされてＣＰＵ５１により実行される。なお、本実施例では、認証用プログラムをＣＤ－ＲＯＭ６３により提供するようにしたが、フロッピーディスク、光磁気ディスク、他の光ディスクなど他の記録媒体で提供するようにしてもよい。また、サーバからネットワーク５を介して提供するようにしてもよい。

【００２９】通信コントローラ５９は、ネットワーク５との通信制御を行うものであり、端末装置２からのアクセス要求を受信するとともに、認証処理時には携帯端末装置３に認証情報を送信する。

【００３０】認証情報データベース６０には、少なくともアクセス元ＩＤ（Identification）情報６１、送信先情報６２が予め記憶されている。アクセス元ＩＤ情報６１は、ユーザを識別するための識別情報である。送信先情報６２は、認証情報を送信すべき先の情報であり、例えば、携帯端末装置３の電話番号である。

【００３１】認証処理時には、認証情報データベース６０に予め記憶された上記アクセス元ＩＤ情報６１、送信先情報６２に基づいて認証処理が実行される。

【００３２】なお、ＲＯＭ５３には、ＢＩＯＳ（Basic Input/Output System）が記憶されている。また、表示装置５７は、表示コントローラ５８により制御され、文字やグラフィックスなどの表示を行なう。

【００３３】次に本実施例の認証処理について説明する。

【００３４】図５に本発明の第１実施例の認証処理の動作説明図を示す。

【００３５】端末装置２でステップＳ１－１でサーバ４にアクセス要求するための操作が行なわれると、端末装置２は、ステップＳ１－２でネットワーク５のうち図１に実線で示す第１の通信経路を介してサーバ４にアクセス要求を送信する。このとき、第１の通信経路は、例えば、一般電話回線網である。

【００３６】サーバ４は、ステップＳ２－１で端末装置２からアクセス要求を受信すると、ステップＳ２－２で第１の通信経路を介して端末装置２にユーザＩＤ、及び、パスワードの入力を要求する。

【００３７】端末装置２は、ステップＳ１－３でサーバ４からのユーザＩＤ、及び、パスワードの入力の要求を受信すると、ユーザＩＤ及びパスワードが手動又は自動で生成され、ステップＳ１－４でネットワーク５を介してサーバ４に送信される。

【００３８】サーバ４は、ステップＳ２－３でユーザＩＤ及びパスワードを受信すると、ステップＳ２－４で受信したユーザＩＤ及びパスワードが予め登録されたものと一致するか否かを判定する。ステップＳ２－４で端末装置２から供給されたユーザＩＤ及びパスワードがサーバ４に予め登録されたユーザＩＤ及びパスワードと一致すれば、入力されたユーザＩＤ及びパスワードは正しいと判定されて、ステップＳ２－５で認証情報を作成する。

【００３９】認証情報は、サーバ４で任意に作成されるキーワードとサーバ４の端末装置２が接続されているポート情報と接続された時間とを合成したものである。なお、ポート情報は、例えばサーバ４のＩＰアドレスであり、特定のサーバで認証が行なわれたことが証明できるものであればよい。また、ここでは、認証情報をポート情報及び接続時間情報とを合成して作成しているが、これに限定されるものではなく、端末装置２からの接続を個別に識別できるものであればよい。

【００４０】作成された認証情報は、ステップＳ２－５で、サーバ４内に記憶されるとともに、認証データベース６０の送信先として登録された携帯端末装置３に送信される。さらに、ステップＳ２－６で認証情報のうちポート情報及び接続時間情報を端末装置２に通知する。

【００４１】このとき、サーバ４と携帯端末装置３との通信は、図１に実線で示す端末装置２とサーバ４との第１の通信経路とは異なる図１に破線で示す第２の通信経路を介して行なわれる。例えば、携帯端末装置３とサーバ４とは、移動通信網を介して通信が行なわれ、端末装置２とサーバ４とは、インターネットと一般回線網を介して通信が行なわれる。なお、サーバ４と携帯端末装置３との通信は、端末装置２とサーバ４との通信とは同じ系統のネットワーク、例えば、一般回線網を用いたとしても一般回線網のうちで通信経路が異なればよい。

【００４２】なお、サーバ４は、ステップＳ２－７で所定時間、端末装置２からユーザＩＤ及びパスワードが供給されないと判定した場合には、ステップＳ２－８で端末装置２にエラー通知を行なう。端末装置２は、ステップＳ１－５でサーバ４からエラー通知を受信すると、サーバ４へのアクセスはエラーとされる。

【００４３】なお、携帯端末装置３は、ステップＳ３－１で、ケーブル２２で端末装置４に接続されるとともに、認証モードとされている。携帯端末装置３は、ステップＳ３－２で、認証情報を受信すると、ステップＳ３－３で受信した認証情報を端末装置４にケーブル２２を介して送信する。なお、端末装置２と携帯端末装置３との通信を赤外線通信あるは無線通信で行なう場合には、ケーブル２２での接続は不要となる。

【００４４】端末装置２は、ステップＳ１－６でサーバ４への接続時にサーバ４のポート情報と接続時間情報を受信しており、ステップＳ１－７で携帯端末装置３から認証情報を受信すると、ステップＳ１－８で携帯端末装置３から受信した認証情報と、サーバ４から受信した接続ポート番号情報及び接続時間情報とを比較し、一致するか否かを判定する。ステップＳ１－８で認証情報とサーバ４から受信したポート情報及び接続時間情報とが一致する場合には、ステップＳ１－９で認証情報をサーバ４にネットワーク５のうちの図１に実線で示す第１の通信経路を介して送信する。また、ステップＳ１－８で認証情報とサーバ４から受信した接続ポート番号情報及び接続時間情報とが不一致の場合には、ステップＳ１－１０でサーバ４にエラー通知が送信され、認証処理は中断される。また、ステップＳ１－６でサーバ４からポート番号情報及び接続時間情報を受信できない場合にもステップＳ１－１０でサーバ４にエラー通知が送信される。なお、サーバ４は、ステップＳ２－１３で端末装置２からエラー通知を受信すると、端末装置２からのアクセスを不許可する。このように、端末装置２側で接続ポート番号情報及び接続時間情報を受信し、携帯端末装置３から供給された認証情報と比較することによりユーザ側でサーバ４の認証を行なえる。このため、悪質なサーバからの保護を行なうことができる。

【００４５】サーバ４は、ステップＳ２－９で端末装置２から認証情報を受信すると、ステップＳ２－１０で端末装置２から受信した認証情報とステップＳ２－５で携帯端末装置３に送信した認証情報とを比較し、一致するか否かを判定する。ステップＳ２－１０で、認証情報が一致した場合には、携帯端末装置３と端末装置２とがケーブル２２により接続されていると判定でき、携帯端末装置３の所有者であるユーザが端末装置２からサーバ４にアクセスを要求していると判定できるため、ステップＳ２－１１で端末装置２にアクセスを許可し、ステップＳ２－１２で端末装置２にアクセス許可通知を送信する。

【００４６】端末装置２は、ステップＳ１－１１でサーバ４からアクセス許可通知を受信すると、サーバ４にアクセスしてサービスを享受することができる。

【００４７】本実施例によれば、ユーザＩＤ及びパスワードを知っているだけではサーバ４にアクセスできず、アクセスするためには携帯端末装置３が必要となる。よって、第三者が他人のユーザＩＤ及びパスワードを使ってサーバ４にアクセスすることを防止できる。

【００４８】なお、本実施例では、端末装置２と携帯端末装置３とのデータ通信をケーブル２２により行なっているが、ＩｒＤＡ方式などの赤外線通信や無線通信によりデータ通信を行なうようにしてもよい。

【００４９】また、本実施例では、認証情報を端末装置２のサーバ４への接続ポート情報並びに時刻情報を合成して生成しているが、サーバ４に予めアクセスする位置情報を登録するとともに、携帯端末装置３に位置情報検出装置を内蔵し、携帯端末装置３から端末装置２を介して位置情報を送信し、位置情報の一致を認証条件に付加することにより、認証を正確に行なえる。

【００５０】図６に本発明の第２実施例のブロック構成図を示す。同図中、図１と同一構成部分には同一符号を付し、その説明は省略する。

【００５１】本実施例のシステム１００は、サーバ１１１の認証情報データベース１１２のデータ構成及び携帯端末装置１１３の構成が相違する。

【００５２】認証情報データベース１１２のデータ構成は、図１に示す認証情報データベース６０に位置情報１１４が付加された点で相違する。また、携帯端末装置１１３は、位置情報検出装置１１５を有する点で携帯端末装置２とは相違する。

【００５３】位置情報検出装置１１５は、例えば、ＧＰＳ（Global Positioning System）による測位装置から構成されている。位置情報検出装置１１５は、携帯端末装置１１３が認証モードのときに、ＧＰＳ衛星１２１からの電波を受信することにより携帯端末装置１１３の位置を検出することが可能な構成とされている。位置情報検出装置１１５で検出された位置情報は、サーバ１１１から認証情報を受信したときに、受信した認証情報に付加される。

【００５４】図７に本発明の第２実施例の認証処理の動作説明図を示す。同図中、図５と同一ステップには同一符号を付し、その説明は省略する。

【００５５】本実施例の認証処理は、携帯端末装置１１３の処理にステップＳ３－１１、Ｓ３－１２を付加するとともに、サーバ１１１の処理にステップＳ２－２１を付加してなる。ステップＳ３－１１は、ステップＳ３－１で認証モードとされたときに、位置検出装置１１５により位置を検出するステップである。ステップＳ３－１２は、ステップＳ３－２で携帯端末装置１１３にサーバ１１１から認証情報が受信されたときに、ステップＳ３－１１で位置情報検出装置１１５により検出された位置情報をサーバ１１１からの認証情報に付加して端末装置２に送信するステップである。

【００５６】ステップＳ２－２１では、位置情報検出装置１１５で検出された位置情報と認証情報データベース１１２に予め登録された位置情報とを比較し、位置情報検出装置１１５で検出された位置情報が認証情報データベース１１２に予め登録された位置情報を中心として所定の範囲内に存在するときには、正当であると判定し、位置情報検出装置１１５で検出された位置情報が認証情報データベース１１２に予め登録された位置情報を中心とした所定の範囲外のときには、正当でないと判定する。

【００５７】ステップＳ２－２１で位置が正当でないと

判定された場合には、ステップＳ２－７で端末装置２にエラーが通知され、端末装置２のサーバ１１１へのアクセスは拒否される。

【００５８】本実施例によれば、携帯端末装置１１３及び端末装置２が認証情報データベース１１２に予め登録された位置情報を中心とした所定の範囲内にあるときに、サーバ１１１へのアクセスが承認される。このため、自宅など所定の場所でしかアクセスが許可されなくなる。よって、第三者が不正にアクセスしようとすると、ユーザの自宅に侵入する必要があるので、容易に不正アクセスを行うことはできない。

【００５９】また、本実施例では、サーバ４が携帯端末装置１１２の位置情報を認識することができ、この位置情報を用いることによりＳＯＨＯ（small office home office）にて勤務している者の　勤務状況の把握に有効となる。また、行政上の申請や届出の際の認証などにも有効となる。

【００６０】なお、上記第１及び第２実施例では、パーソナルコンピュータによるサーバ４へのアクセスのための認証方式に本発明の認証方式を用いたが、クレジットカードの端末や自動販売機などの不正使用を防止するために本発明の認証方式を用いるようにしてもよい。

【００６１】図８に本発明の第３実施例のブロック構成図、図９に本発明の第３実施例の動作説明図を示す。同図中、図１、図５と同一構成部分には同一符号を付し、その説明は省略する。

【００６２】本実施例のシステム２００は、買い物の支払いをクレジットカード２０１で行なう際に使用されるシステムである。本実施例のシステム２００で使用されるクレジットカード読取装置２０２には、第１実施例の端末装置２に相当する機能が組み込まれている。

【００６３】クレジットカード２０１で支払いを行なう場合に、携帯端末装置３をカード読取装置２０２にケーブル２２により接続し、携帯端末装置３の動作モードを認証モードにする。カード読取装置２０２は、ステップＳ１－３１でクレジットカード２０１が読み取られると、ネットワーク５のうち図８に実線で示す第１の通信経路を介してサーバ４にアクセス要求を行なう。

【００６４】サーバ４は、カード読取装置２０２からアクセス要求があると、カード読取装置２０２に対してユーザＩＤ及びパスワードの入力を要求する。クレジットカード２０１の使用者によりユーザＩＤ及びパスワードの入力が行なわれると、カード読取装置２０２は、図８に実線で示す第１の通信経路を介してサーバ４にユーザＩＤ及びパスワードを送信する。

【００６５】なお、ユーザＩＤ及びパスワードは入力するのではなくクレジットカードから提供されるようにしてもよい。

【００６６】サーバ４は、カード読取装置２０２からネットワーク５のうち図８に実線で示す第１の通信経路を介してアクセス要求があり、ユーザＩＤ及びパスワードが承認されると、第１実施例と同様に図８に破線で示す第２の通信経路を介して携帯端末装置３に認証情報を送信する。携帯端末装置３も第１実施例と同様に認証情報をカード読取装置２０２にケーブル２２、赤外線通信、無線通信などにより送信する。

【００６７】カード読取装置２０２は、携帯端末装置３から認証情報を受信すると、ネットワーク５のうち図８に実線で示す第１の通信経路を介してサーバ４に認証情報を送信する。サーバ４は、第１実施例と同様に端末装置２からの認証情報を携帯端末装置３に送信した認証情報と比較して、一致したときには、ステップＳ２－３１で商品の代金に対応した金額を予め登録された口座から引き落とし、ステップＳ２－３２でカード読取装置２０２に支払い完了通知を送信する。

【００６８】カード読取装置２０２では、サーバ４から支払い完了通知を受信すると、ステップＳ１－１２で支払いが完了した旨の通知を行なう。

【００６９】本実施例によれば、ユーザＩＤ及びパスワード並びに携帯端末装置を所持したユーザだけがクレジットカード２０１を使用することができ、クレジットカード２０１の不正使用が困難となる。

【００７０】図１０に本発明の第４実施例のブロック構成図、図１１に本発明の第４実施例の動作説明図を示す。同図中、図１、図５と同一構成部分には同一符号を付し、その説明は省略する。

【００７１】本実施例のシステム３００は、自動販売器３０１での支払いを行なう際に使用される認証システムである。本実施例のシステム３００で使用される自動販売機３０１には、第１実施例の端末装置２に相当する機能が組み込まれている。

【００７２】自動販売機３０１で支払いを行なう場合に、携帯端末装置３の動作モードを認証モードにする。自動販売機３０１は、ステップＳ１－４１で商品が選択されると、サーバ４にアクセス要求を行なう。サーバ４は、自動販売機３０１からアクセス要求があると、自動販売機３０１に対してユーザＩＤ及びパスワードの入力を要求する。商品の購入者により自動販売機３０２に設けられたキーボード３０２によりユーザＩＤ及びパスワードの入力が行なわれると、自動販売機３０１は、サーバ４にユーザＩＤ及びパスワードを送信する。

【００７３】なお、ユーザＩＤ及びパスワードは入力するのではなくカードなどにより提供されるようにしてもよい。

【００７４】サーバ４は、自動販売機３０１からネットワーク５のうち図１０に実線で示す第１の通信経路を介してユーザＩＤ及びパスワードが入力され、ユーザＩＤ及びパスワードが承認されると、第１実施例と同様に図１０に破線で示す第２の通信経路を介して携帯端末装置３に認証情報を送信する。携帯端末装置３も第１実施例

と同様に認証情報を自動販売機３０１にケーブル２２、赤外線通信、無線通信などにより送信する。

【００７５】自動販売機３０１は、携帯端末装置３から認証情報を受信すると、ネットワーク５のうち図１０に実線で示す第１の通信経路を介してサーバ４に認証情報を送信する。サーバ４は、第１実施例と同様に端末装置２からの認証情報を携帯端末装置３に送信した認証情報と比較して、一致したときには、ステップＳ２－３１で商品の代金に対応した金額を予め登録された口座から引き落とし、ステップＳ２－３２で自動販売機３０１に支払い完了通知を送信する。自動販売機３０１では、サーバ４から支払い完了通知を受信すると、ステップＳ１－４２で商品を自動販売機３０１の取出口３０３より排出する。

【００７６】本実施例によれば、ユーザＩＤ及びパスワード並びに携帯端末装置を所持したユーザだけが自動販売機３０１で商品を入手することができ、不正使用が困難となる。また、自動販売機に現金を置く必要がないので、防犯上も好適となる。

【００７７】なお、第１～第４実施例では、認証情報の送信先として携帯電話などの携帯端末装置３を例として説明したが、認証情報の送信先は、端末装置２とサーバ４との通信経路と異なっていればよく、通常の端末装置であってもよい。

【００７８】なお、本発明の認証システムは、上記実施例に限定されるものではなく、本発明の請求の範囲を逸脱しない範囲で種々の変形例が可能である。

【００７９】

【発明の効果】上述の如く、本発明によれば、ユーザＩＤやパスワードを知っているだけでは第１の端末装置は認証されることはなく、第１の端末装置と第２の端末装置とを組み合わせて使用する必要があるため、ユーザＩＤやパスワードの不正使用が困難になるなどの特長を有する。

【００８０】本発明によれば、第２の端末装置で位置情報を付加することにより、第１の端末装置が認証装置に予め登録された位置に対応する位置にあるときに、第１の端末装置の正当性が判定されるので、ユーザＩＤやパスワードの不正使用をさらに困難にできるなどの特長を有する。

【図面の簡単な説明】

【図１】本発明の第１実施例のシステム構成図である。

【図２】本発明の第１実施例の端末装置のブロック構成図である。

【図３】本発明の第１実施例の携帯端末装置のブロック構成図である。

【図４】本発明の第１実施例のサーバのブロック構成図である。

【図５】本発明の第１実施例の動作説明図である。

【図６】本発明の第２実施例のブロック構成図である。

【図７】本発明の第２実施例の動作説明図である。

【図８】本発明の第３実施例のブロック構成図である。

【図９】本発明の第３実施例の動作説明図である。

【図１０】本発明の第４実施例のブロック構成図である。

【図１１】本発明の第４実施例の動作説明図である。

【符号の説明】

１，１００，２００，３００　認証システム

２　端末装置

３　携帯端末装置

４，１１１　サーバ

５　ネットワーク

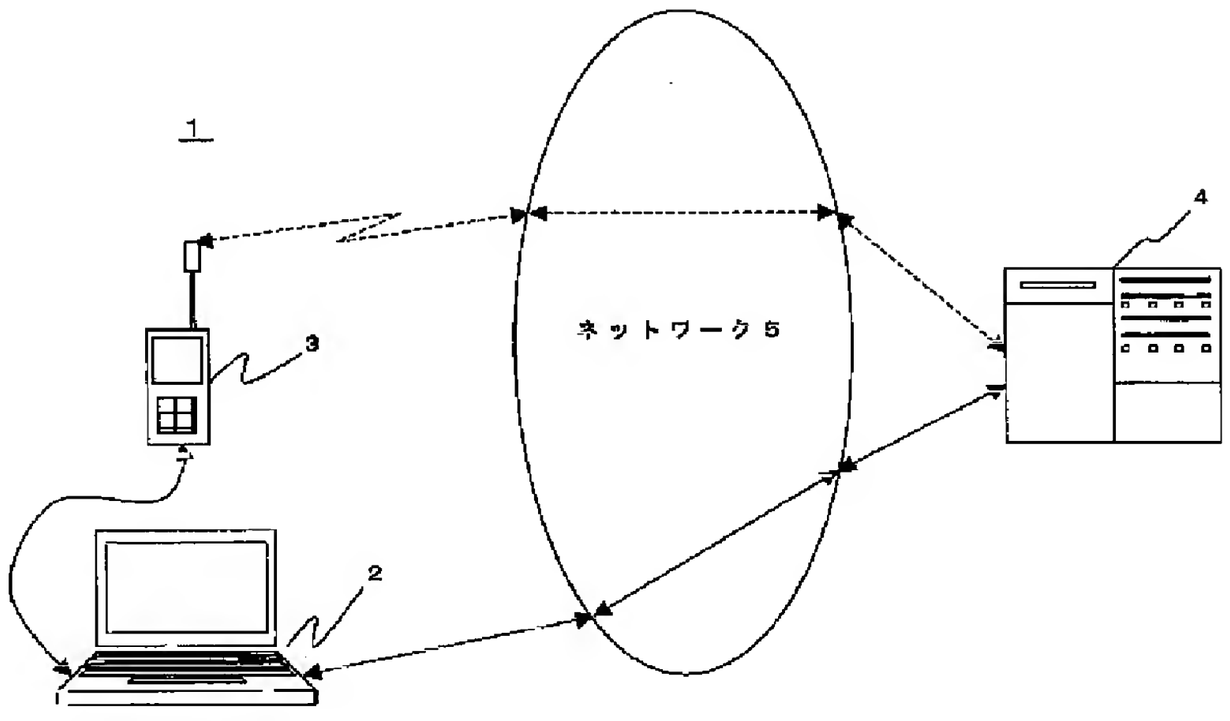
６０、１１２　認証情報データベース

６１　アクセス元ＩＤ

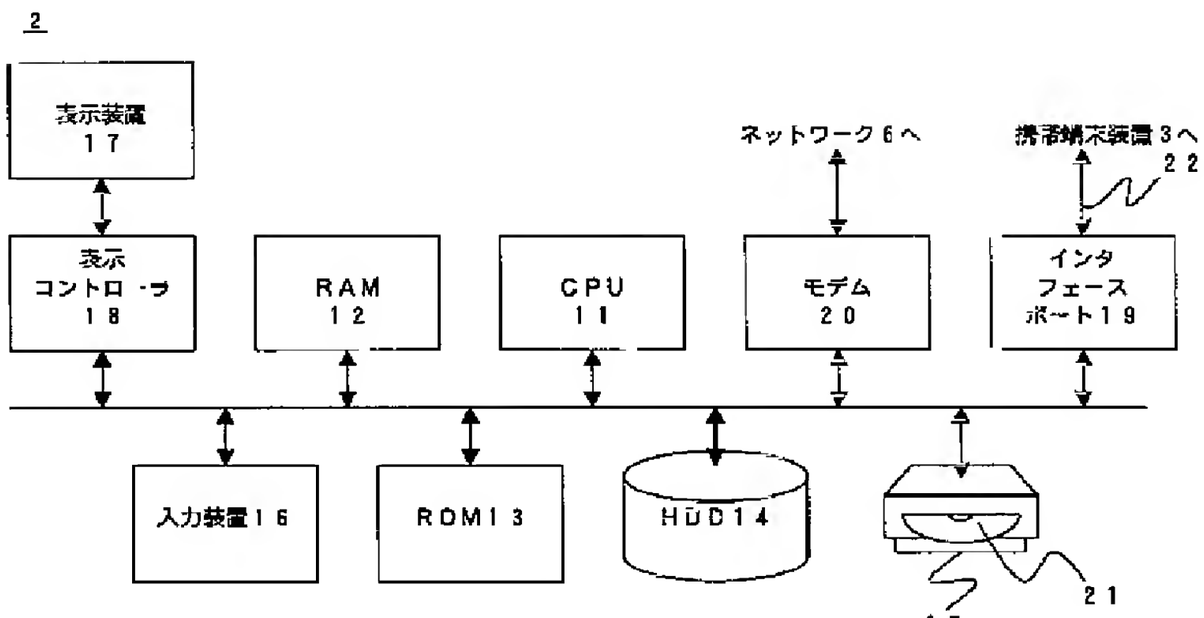
６２　送信先情報

１１４　位置情報

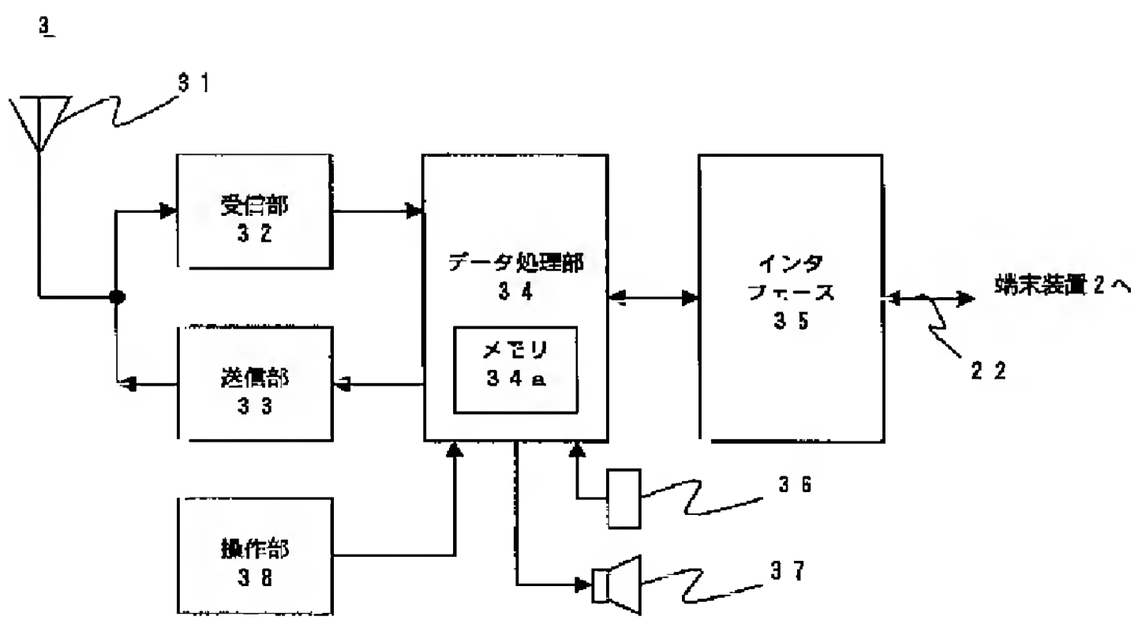
【図１】



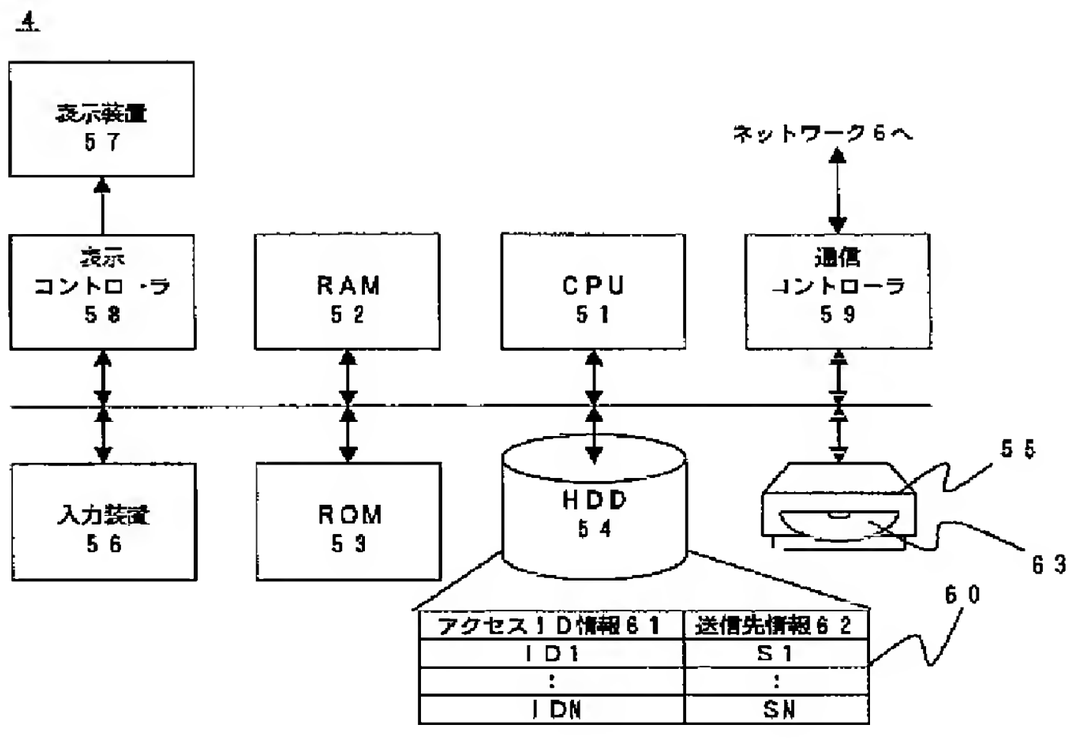
【図２】

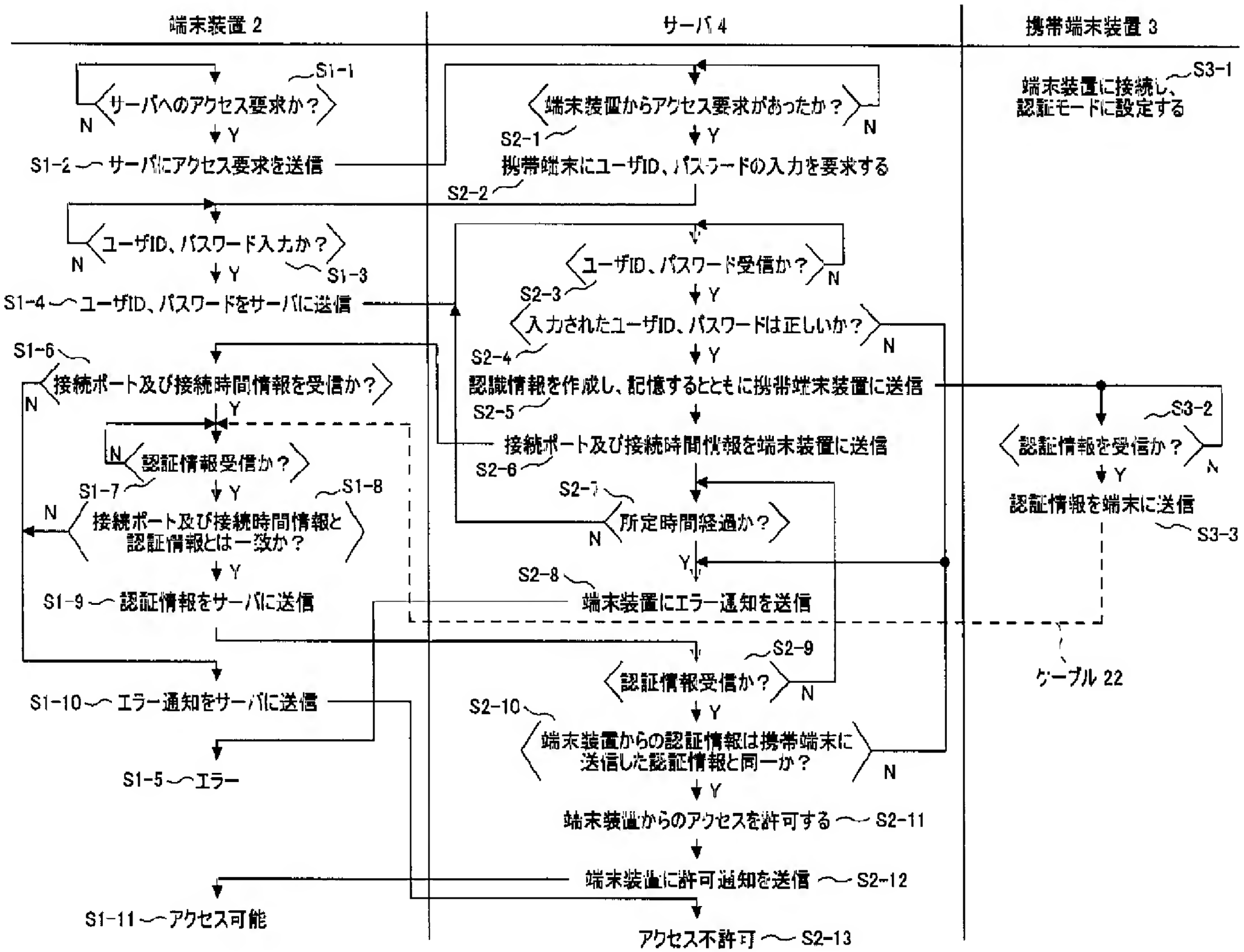

2
表示装置
17
表示
コントロ ーラ
18
RAM
12
CPU
11
ネットワーク6へ
モデム
20
携帯端末装置3へ
22
インタ
フェース
ポート19
入力装置16
ROM13
HDD14
21
15

【図３】


3
31
受信部
32
送信部
33
データ処理部
34
メモリ
34a
インタ
フェース
35
端末装置2へ
22
36
37
操作部
38

【図４】

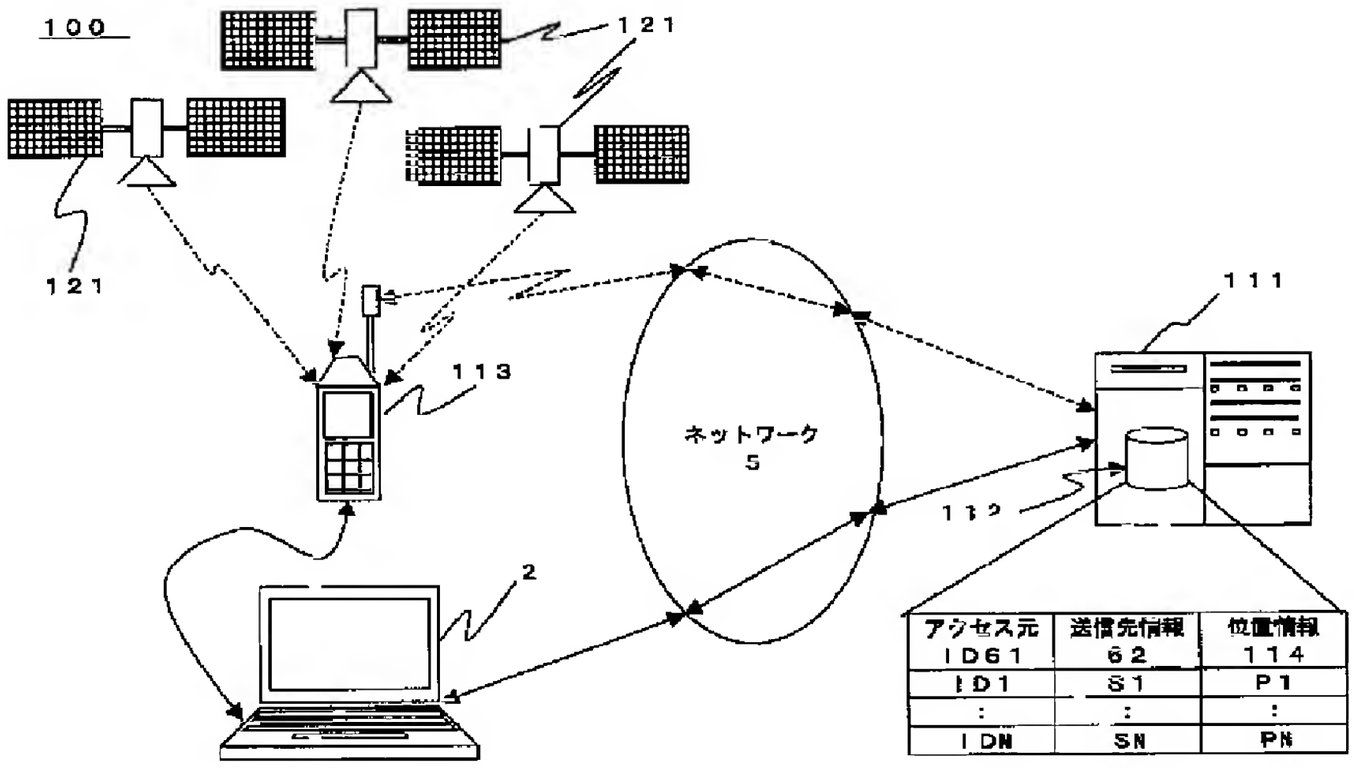

4
表示装置
57
表示
コントロ ーラ
58
RAM
52
CPU
51
ネットワーク6へ
通信
コントローラ
59
入力装置
56
ROM
53
HDD
54
55
63
60
アクセスID情報61
送信先情報62
ID1
S1
:
:
IDN
SN



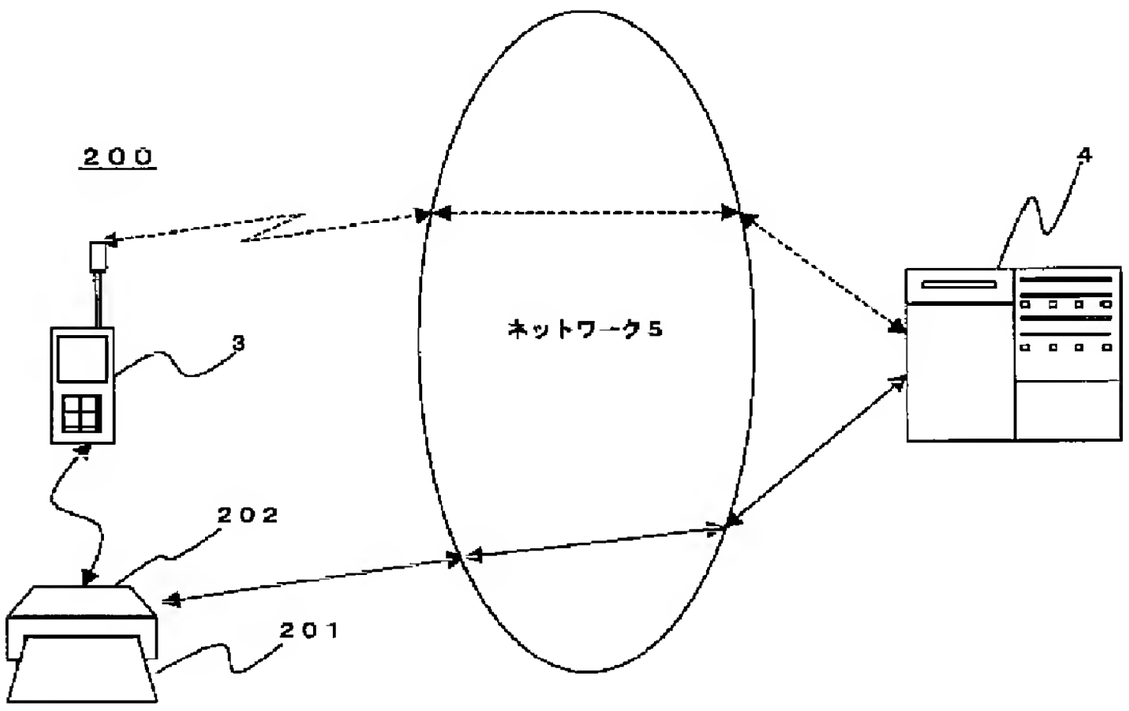
【図5】

(9) 002-140302 (P2002-140302A)

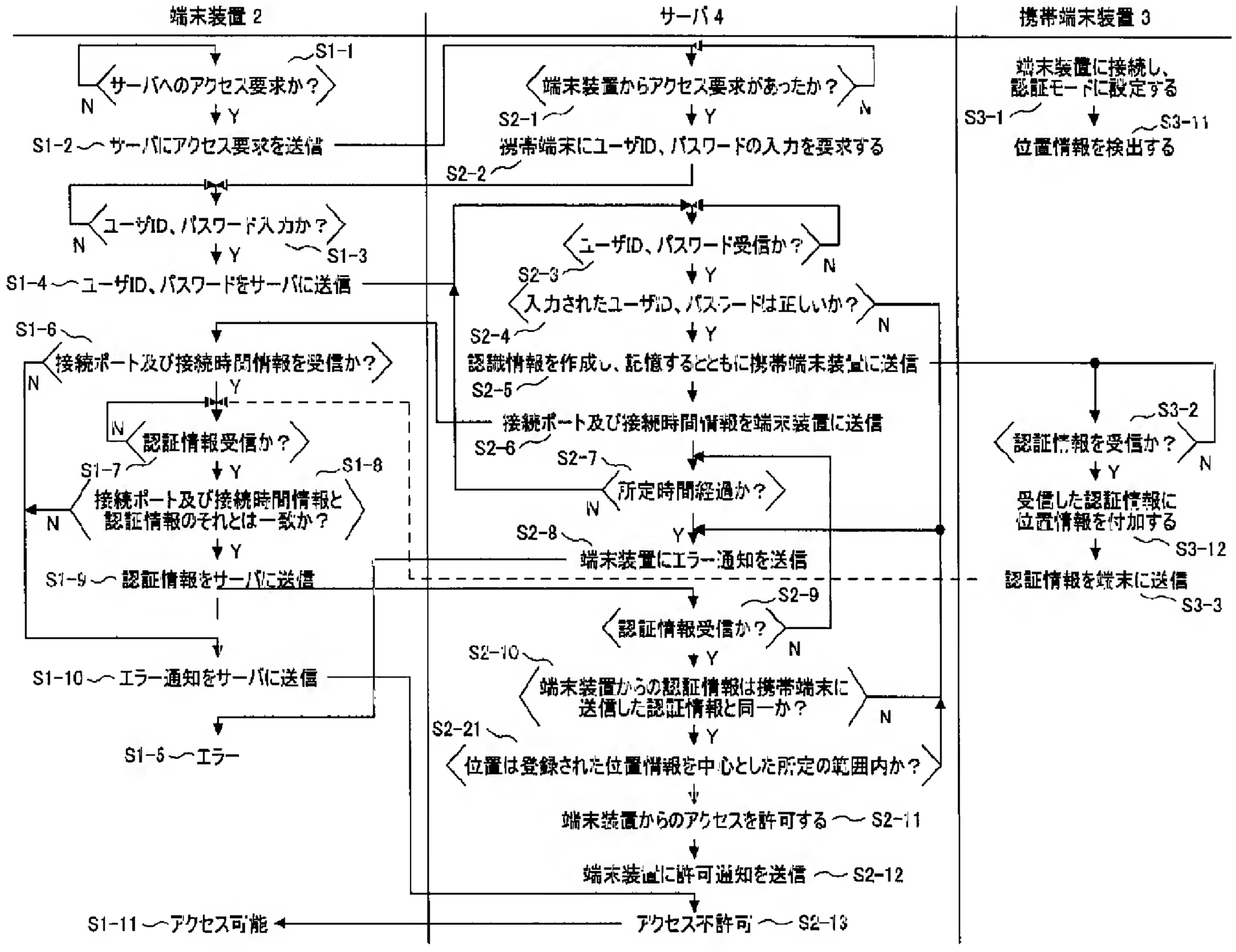
【図6】

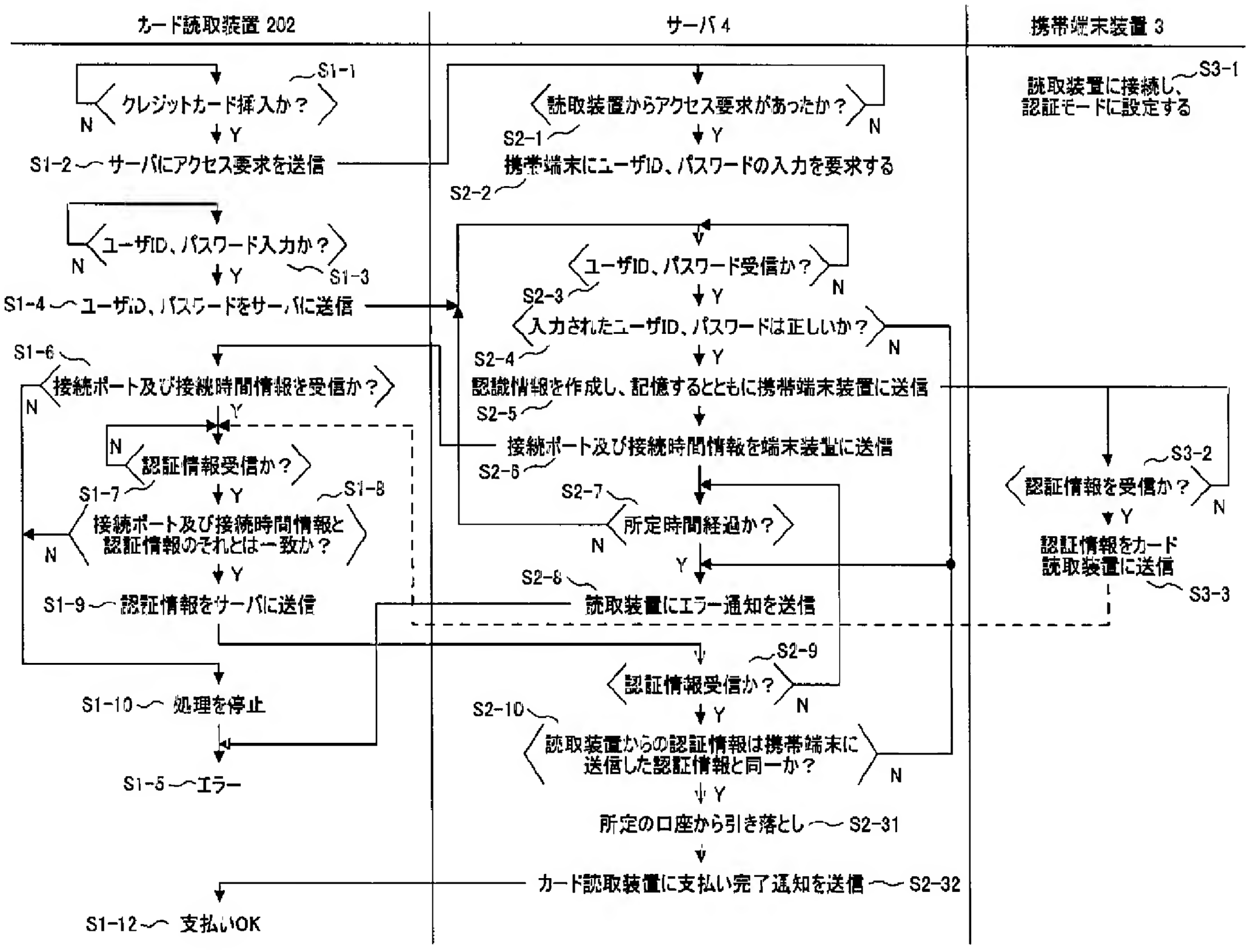

100
121
121
113
ネットワーク
5
111
112
2
アクセス元
ID61
送信先情報
62
位置情報
114
ID1
S1
P1
:
:
:
IDN
SN
PN

【図8】


200
ネットワーク5
4
3
202
201

【図7】

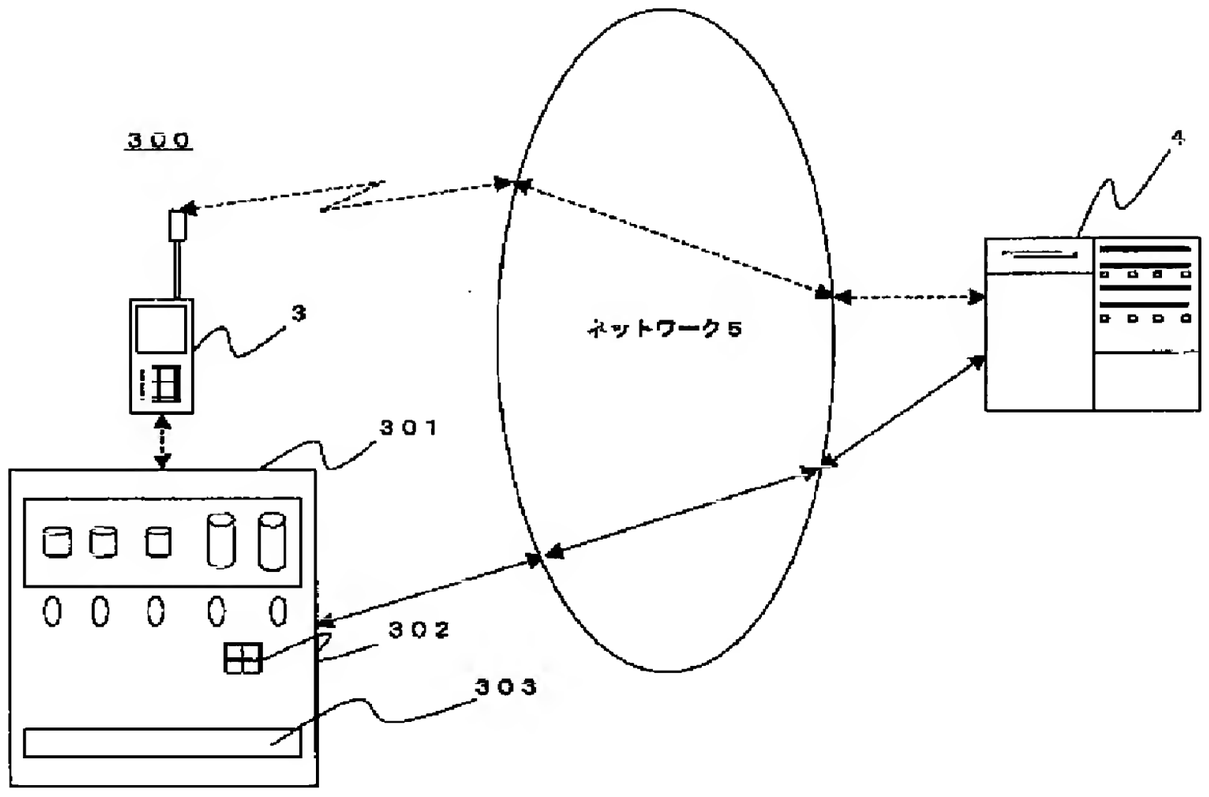

端末装置 2
サーバ 4
携帯端末装置 3
S1-1
サーバへのアクセス要求か？
N
Y
S1-2 サーバにアクセス要求を送信
S1-3
ユーザID、パスワード入力か？
S1-4 ユーザID、パスワードをサーバに送信
S1-6
接続ポート及び接続時間情報を受信か？
認証情報受信か？
S1-7
S1-8
接続ポート及び接続時間情報と認証情報のそれとは一致か？
S1-9 認証情報をサーバに送信
S1-10 エラー通知をサーバに送信
S1-5 エラー
S1-11 アクセス可能
端末装置からアクセス要求があったか？
S2-1
携帯端末にユーザID、パスワードの入力を要求する
S2-2
ユーザID、パスワード受信か？
S2-3
入力されたユーザID、パスワードは正しいか？
S2-4
認識情報を作成し、記憶するとともに携帯端末装置に送信
S2-5
接続ポート及び接続時間情報を端末装置に送信
S2-6
S2-7
所定時間経過か？
S2-8
端末装置にエラー通知を送信
S2-9
認証情報受信か？
S2-10
端末装置からの認証情報は携帯端末に送信した認証情報と同一か？
S2-21
位置は登録された位置情報を中心とした所定の範囲内か？
端末装置からのアクセスを許可する S2-11
端末装置に許可通知を送信 S2-12
アクセス不許可 S2-13
端末装置に接続し、認証モードに設定する
S3-1
S3-11
位置情報を検出する
S3-2
認証情報を受信か？
受信した認証情報に位置情報を付加する
S3-12
認証情報を端末に送信
S3-3



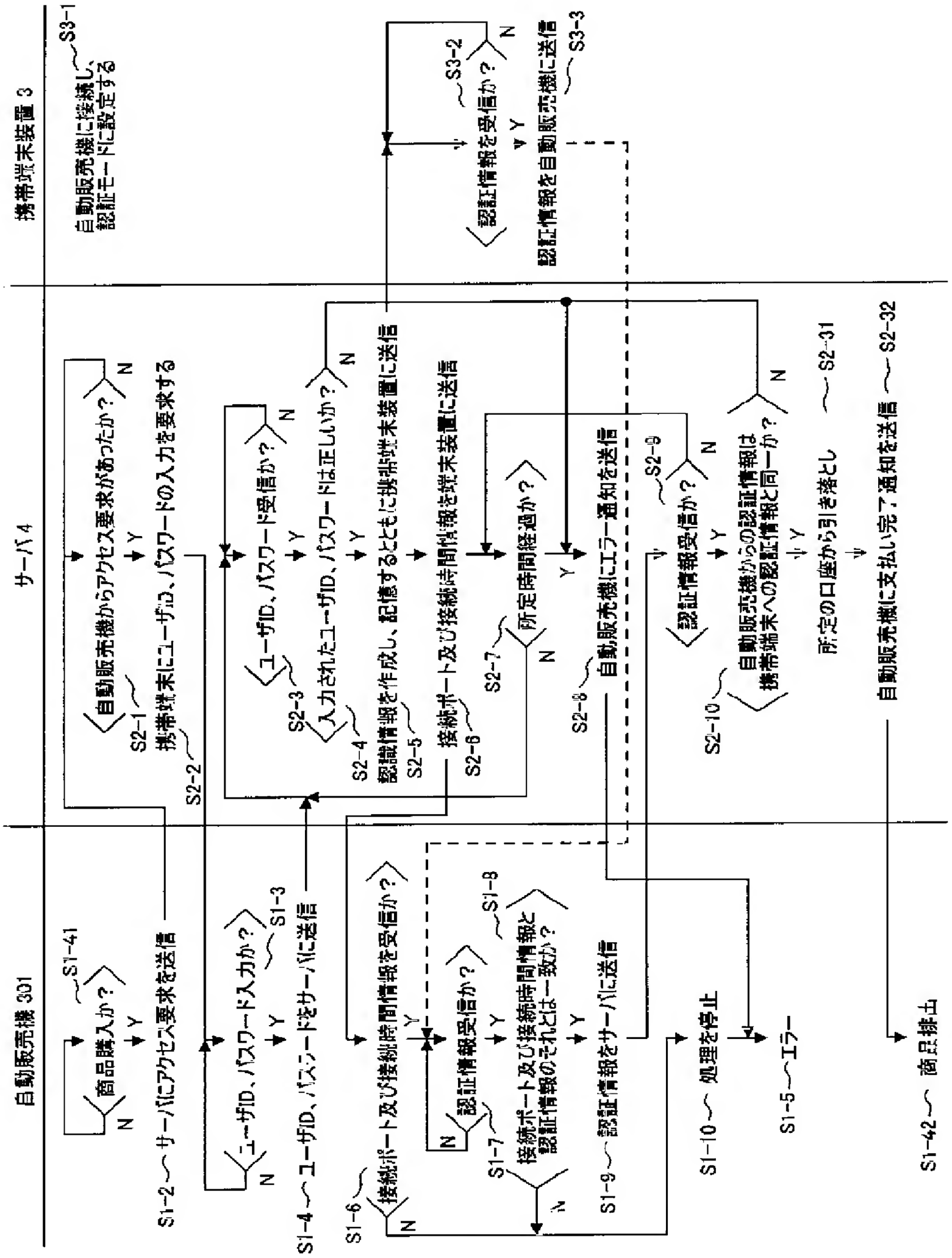
【図9】

(丸2))02-140302(P2002-140302A)

【図10】



【図11】


携帯端末装置 3
サーバ 4
自動販売機 301
S3-1
自動販売機に接続し、認証モードに設定する
S3-2
認証情報を受信か？
N
Y
S3-3
認証情報を自動販売機に送信
S2-1
自動販売機からアクセス要求があったか？
S2-2
携帯端末にユーザID、パスワードの入力を要求する
S2-3
ユーザID、パスワード受信か？
S2-4
入力されたユーザID、パスワードは正しいか？
S2-5
認証情報を作成し、記憶するとともに携帯端末装置に送信
S2-6
接続ポート及び接続時間情報を端末装置に送信
S2-7
所定時間経過か？
S2-8
自動販売機にエラー通知を送信
S2-9
認証情報受信か？
S2-10
自動販売機からの認証情報は携帯端末への認証情報と同一か？
S2-31
所定の口座から引き落とし
S2-32
自動販売機に支払い完了通知を送信
S1-41
商品購入か？
S1-2 サーバにアクセス要求を送信
S1-3
S1-4 ユーザID、パスワードをサーバに送信
S1-6
接続ポート及び接続時間情報を受信か？
S1-7
認証情報受信か？
S1-8
接続ポート及び接続時間情報と認証情報のそれとは一致か？
S1-9 認証情報をサーバに送信
S1-10 処理を停止
S1-5 エラー
S1-42 商品排出